

# EXHIBIT 8

# Freedom to Tinker

... is your freedom to understand, discuss, repair, and modify the technological devices you own.

---

« [CD DRM Makes Computers Less Secure](#)  
[SonyBMG and First4Internet Release Mysterious Software Update](#) »

## CD-DRM Rootkit: Repairing the Damage

Wednesday November 2, 2005 by Ed Felten

SonyBMG and First4Internet are in the doghouse now, having been caught installing [rootkit-like software](#) on the computers of SonyBMG music customers, thereby exposing the customers to security risk. The question now is whether the companies will face up to their mistake and try to remedy it.

First4Internet seems to be trying to dodge the issue. For example, here's part of a news.com [story](#) by John Borland:

The creator of the copy-protection software, a British company called First 4 Internet, said the cloaking mechanism was not a risk, and that its team worked closely with big antivirus companies such as Symantec to ensure that was the case. The cloaking function was aimed at making it difficult, though not impossible, to hack the content protection in ways that have been simple in similar products, the company said.

In any case, First 4 has moved away from the techniques used on the Van Zant album to new ways of cloaking files on a hard drive, said Mathew Gilliat-Smith, the company's CEO.

"I think this is slightly old news," Gilliat-Smith said. "For the eight months that these CDs have been out, we haven't had any comments about malware (malicious software) at all."

The claim that the software is not a risk is simply false, as Alex [explained](#) yesterday. And if the company is indeed working on new ways to hide the contents of your computer from you, that just shows that they haven't learned their lesson. The problem is not that they used a particular rootkit method. The problem is that they used rootkit methods at all. Switching to a new rootkit method will, if anything, make the problem worse.

The claim that there haven't been any complaints about the software is also false. The reviews on Amazon have plenty of complaints, and there was a [discussion](#) of these problems at CastleCops. And, of course, Mark Russinovich has complained.

The claim that this is old news is just bizarre. First4Internet is offering this system to record companies — today. SonyBMG is selling CDs containing this software — today. And this software is sitting on many users' computers with no uninstaller — today.

If the First4Internet wants to stop spinning and address the problem, and if SonyBMG wants to start recovering consumer trust, I would suggest the following steps.

(1) Admit that there is a problem. The companies can admit that the software uses rootkit-like methods and may expose some consumers to increased security risk.

(2) Modify product packaging, company websites, and EULA language to disclose what the software actually does. Thus far there hasn't been adequate notification. For example, the current EULA says this:

As soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically install a small proprietary software program (the "SOFTWARE") onto YOUR COMPUTER. The SOFTWARE is intended to protect the audio files embodied on the CD, and it may also facilitate your use of the DIGITAL CONTENT. Once installed, the SOFTWARE will reside on YOUR COMPUTER

until removed or deleted. However, the SOFTWARE will not be used at any time to collect any personal information from you, whether stored on YOUR COMPUTER or otherwise.

Clearly a rootkit neither protects the audio files nor facilitates use of the content. This is not the only misleading aspect of the description. For example, this does not convey to users that they will be unable to make lawful uses of the music such as downloading it to an iPod, or that there is no way to uninstall the software (indeed, it strongly implies the opposite), or that attempting to remove the software may make the computer's CD drive inaccessible.

(3) Release a patch or uninstaller that lets any consumer easily remove or disable the rootkit-like functions of the software. Having caused security problems for their users, the least the companies can do is to help users protect themselves.

(4) Make clear that the companies support, and give permission for, research into the security implications of their products. Saying "trust us" won't cut it anymore. Having betrayed that trust once, the companies should publicly welcome the Mark Russinoviches of the world to keep studying their software and publishing what they find. If you act like you have something to hide — and you have had something to hide in the past — the public will be smart enough to conclude that you're probably still hiding something. This is especially true if you announce that you are trying to find new ways to do the thing that you were just caught doing!

Finally, let me just point out two things. First, we don't know yet whether the First4Internet/SonyBMG software causes even more security or privacy problems for users. Given what we've seen so far, I wouldn't be at all surprised if there are more problems lurking.

Second, this general issue applies not only to F4I and SonyBMG's technology. Any attempt to copy-protect CDs will face similar problems, because this kind of copy-protection software has a lot in common with standard malware. Most notably, both types of software try to maintain themselves on a user's computer against the user's will — something that cannot be done without eroding the user's control over the computer and thereby inhibiting security.

If you're using a recent version of Windows, you can protect yourself against this type of software, and some other security risks, by [disabling autorun](#).

This entry was posted on Wednesday November 2, 2005 at 7:58 am and is filed under [Security](#), [DRM](#), [CD Copy Protection](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.

#### **Ubeatable Copy Protection**

Alan Technology Technology for Software & Hardware

Ads by Goooooogle

#### **MySpace Turned Inside-Out**

Meet others online, share your pictures, and blog for free.

[Advertise on this site](#)

## **37 Responses to "CD-DRM Rootkit: Repairing the Damage"**

1. *matt* Says:

[November 2nd, 2005 at 9:45 am](#)

or maybe someone in congress could just pass the Digital Media Consumers' Rights Act (<http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.107:>) so that SonyBMG would have to put a big label on the disk that says "this won't work for you!".

2. *Mat Hall* Says:

[November 2nd, 2005 at 10:38 am](#)

*Most notably, both types of software try to maintain themselves on a user's computer against the user's will — something that cannot be done without eroding the user's control over the computer and thereby inhibiting security.*

This is a pretty good summary of the UK Computer Misuse Act, and although IANAL I'd be fairly confident that they could be successfully prosecuted. Any enterprising lawyers out there want to have a go?

3. [Technology & Marketing Law Blog](#) Says:  
November 2nd, 2005 at 11:52 am

### **Sony, DRM and Trespass to Chattels**

By Eric Goldman A minor storm is brewing over Sony's installation of DRM software on users' computers when they play...

4. [NO ONE RECEIVING » fear of a black hat](#) Says:  
November 2nd, 2005 at 1:12 pm

[...] What does Ed Felten think about all this? (aha, I knew he'd say somethin eventually) [...]

5. [tobias robison](#) Says:  
November 3rd, 2005 at 3:48 am

Were Symantec and other virus companies REALLY contacted in the development of this rootkit? If so, why didn't they go public and complain?

There may be a story here, please follow it up!

6. [Tom](#) Says:  
November 3rd, 2005 at 6:46 am

Good post, if a bit pointless. What people do not realize is that big corporations already own us. They have all the power, we don't have any.

Big corporations can do what they want with impunity. There is nothing we can do to stop them. A few posts here and there is not going to stop this steady erosion of our rights. Even a law won't help- SONY and all the rest have billions of dollars to spend; we don't. And sadly, people don't care. Rights that we take for granted are being taken away daily.

One could tell me to write my congressperson- sure. What good is it going to do? Our so-called representatives care less for their constituents rights than they do for money, so we lost again.

Let's face it- we are again serfs and slaves to the mighty- and most of us don't care.

7. [Memex 1.1 » Blog Archive » Sony resorts to malware techniques](#) Says:  
November 3rd, 2005 at 4:27 pm

[...] Fascinating technical analysis by Mark Russinovich of what he discovered happened to his Windows machine when he inserted a copy-protected Sony music disc. Basically, the disc installs the kind of covert software used by malware authors (aka 'hackers' to the mainstream media). Ed Felten has posted several thoughtful updates and comments on this unsavoury discovery. [...]

8. [LC CyberBlog » Blog Archive » Sony/BMG and the DMCA chill](#) Says:  
November 3rd, 2005 at 5:54 pm

[...] The flap over Sony/BMG's DRM is growing. There is a lot of interesting commentary out there on this point. Ed Felten's (yes the same Ed Felten that tried to get a court to decide whether the DMCA prohibited his research efforts as a computer scientist at Princeton investigating the music industries "Secure Digital Music Initiative" or SDMI) has a great set of recommendations for Sony/BMG to rehabilitate itself. I particularly like his recommendations as framed by Donna Wentworth at Copyfights. Much of what he suggests we came up with in our discussions in class. His final recommendation is one we did not talk about: (4) Make clear that the companies support, and give permission for, research into the security implications of their products. Saying "trust us" won't cut it anymore. [...]

9. [TsuDoNymh](#) Says:  
November 4th, 2005 at 9:50 am

The part that interests me most: "The creator of the copy-protection software, a British company called First 4 Internet, said the cloaking mechanism was not a risk, and that its team worked closely with big antivirus companies such as Symantec to ensure that was the case."

Symantec cooperated in not detecting a rootkit on my computers?! Let's get some comments from Symantec on how they worked this.

10. *Malcolm Powell* Says:  
[November 4th, 2005 at 11:33 am](#)

"Tom" wrote: "SONY and all the rest have billions of dollars to spend; we don't".

Tom there are billions of us and a lot of us have a few dollars. They cannot do anything unless we are all apathetic like you and let them.

"Tom" wrote: "Let's face it- we are again serfs and slaves to the mighty- and most of us don't care".

Tom you, and your ilk, are deeply sad and pathetic.

11. *Cyber Crime Law* Says:  
[November 4th, 2005 at 12:17 pm](#)

### **Did Sony CD Malware Violate US Computer Fraud and Abuse Act?**

I think it would be a stretch to say that Sony violated CFAA, but I have to admit that in my opinion they come pretty close. Many readers are well-aware of the scandal of the week in cyberspace - Sony's stealth digital rights management system w

12. *Peter Fusco* Says:  
[November 4th, 2005 at 1:00 pm](#)

As soon as I first read about this I fired off several emails. One to my Congresswoman (haven't gotten anything back yet) and to a lot of friends and co-workers. I also wrote Sony and told them that they have lost me forever as a consumer of their products.

The big corporations DO have more money and more influence in congress than we do, however perhaps it is time to start a IT issue/ consumer rights lobby of our own. More importantly, look to start electing politicians who "understand" what this is all about, who are not close to fossilization. It is time to begin electing IT savvy men and women to office.

13. *IndMusic* Says:  
[November 4th, 2005 at 4:39 pm](#)

Enough is enough. I will no longer purchase any music with copy protection or the use of DRM. Sony's latest copy protection scheme consumes CPU power on my computer alters basic system files and even goes as far as altering the "Safe Boot" mode built into Microsoft Operating System.

RIAA and large recording companies like Sony, BMG is destroying the music industry. They have been slow to adapt to the changing trends that the personal computer is becoming the media portal of choice by many people. They have crippled the quality of music played on computers by building in highly compressed Digit Rights Managed music on the CD they sell. The recording industry is running trials of different restrictions and copy protection programs all of which end up on the user's computer. Inconsistencies in these copy protection schemes are well hidden and rarely identified as the problem when problems do occur.

Before the RIAA began their witch hunts that started around 2001 I was purchasing over 40 music CDs a year. The continued bad taste the recording industry has left me with, has reduced my yearly music CD purchases to

under 8 CD per year. Beginning in 2006 I will no longer purchase any music that uses DRM or any other form of copy preventing software.

When I purchase music I want the ability to play my purchased music on any device I own or that is in my presents. I want the ability to play my purchased music on my computer, in my walkman, on my Ipod. I want the ability to convert my music to a format that supports the device I want to use both now and in the future. I do not want my purchased music to be tied to a single technology. I have already purchased my music at least three times. In the early ages I built up a very large LP collection. Then repurchased my music when 8 tracks became popular and again when cassettes become popular. With the quality improvements of compact discs I set out to purchase my collection again.

Like most people I'm very respectful of the artist and make sure they are rightfully compensated for there music. I am more than glad to purchase my music and in the past have used file sharing as a way to discover new artist. I have stopped using all forms of file sharing in 2002. Since I used file sharing to discover new artist I wanted to protect myself by documenting that all my music in my collection was purchased. My own record keeping has turned up some very interesting trends. My documented trends in my music habits are in direct contrast to what the RIAA claims to be there largest threat.

Call to arms. All independent labels and independent artist please make your self know. I enjoy buying my music via the web and I want it unprotected. I have found the one stop on line music stores to be very convenient. I also have found the "music CD clubs" to be ok and have belonged to as many as four of them at the same time.

It's a real shame that I feel I must offer no more support to the many great artist that are under the Sony, BMG labels. While at the same time I'm excited to discover what the new year will bring to me in the way of undiscovered artist. Over time I hope these independents create large portals to distribute there music via the web.

14. [Chilloutcorner » Blog Archive » Copy protection gone too far](#) Says:  
[November 5th, 2005 at 8:45 am](#)

[...] I don't want to go into details, you can read more about it here, here and here at Freedom to Tinker. It looks like it is a pain to get rid of this software, as soon as the news came out, the rating for the disc at amazon.com went down. [...]

15. [skeptic](#) Says:  
[November 5th, 2005 at 5:43 pm](#)

Peter Fusco said:

"...perhaps it is time to start a IT issue/ consumer rights lobby of our own."

We have one - support the Electronic Frontier Foundation, <http://www.eff.org/> Sign up for their 'Effector' email list, which frequently includes action links. And send money 😊 Disclosure: I have no personal connection to eff.org

16. [BC](#) Says:  
[November 7th, 2005 at 1:23 am](#)

NEW ROOTKIT DISCOVERED (?) (!!!)

A certain CD behaved very strangely as it was played in the computer. The computer went BSOD shortly after displaying symptoms of keylogging and modifying files but until this news broke no one could believe a legitimate CD could have a virus. It was certainly a rootkit, since it was smart enough to type html into my computer-generated-music website HTML code. ...Bfast.com... Spybot identified Bfast as Spyware and removed it but

this CD maybe even sicker than the November 1 2005 announced one.

This CD is JOHN MAYER - HEAVIER THINGS , CD EXTRA FORMAT  
Apparently it's rootkit may be made by "Specific Harm Music (ASCAP)" !!!  
Plenty of other evidence, a sticker saying you'll hear unreleased songs  
only on a computer. I thought that only a few Sony CDs had rootkits since  
March 2005 but this CD is a bit older than that! Other branding: AWARE, COLUMBIA.

Ironically, the only way to remove the ASCAP virus is put it into the Analog Hole!...  
...Which on October 31 was rumored to be assaulted again by the Evil Ones!

17. [\*Edward Kimble\*](#) Says:  
[November 7th, 2005 at 11:23 am](#)

Last time I checked it was a major multidecade jail sentence for hacking. In England even typing ..\\ could land you in jail for 20 years. Sounds like all that is needed here is a 100 million dollar lawsuit with 20 years jail time for each instigator and collaborator. Symantec should know better than to aid hackers and should suffer the jail time perquisit to that stupidity..

18. [\*Mark\*](#) Says:  
[November 7th, 2005 at 10:37 pm](#)

What would happen if another... cough, legitimate, cough music/software company attempted to copy protect their music/software using a similar method. Can two or more rootkits co-exist on the same OS at the same time? I would think there would be all kinds of conflicts as one rootkit attempted to overwrite/block the other(s) rootkids drivers. Oh, what a mess!

19. [\*Blog Interiuris - Andy Ramos » Más DRM, más ataques para los consumidores\*](#) Says:  
[November 8th, 2005 at 2:36 am](#)

[...] Muchos se preguntan en la Red si es legal o no este sistema anticopia ya que está introduciendo en un sistema código potencialmente dañino; la respuesta no es sencilla ya que como os he dicho, no todos los expertos se ponen de acuerdo en qué es exactamente esta aplicación, si un rootkit en sentido estricto, o como opina Edward Ferten del blog Freedom to Tinker, es algo parecido pero no del todo un rootkit. También es importante ver el EULA (End User License Agreement - Acuerdo de Licencia de Usuario Final), ya que si en el mismo se especifica qué se va a instalar en el ordenador, el usuario estaría dando una aceptación tácito al introducir el CD en la bandeja del lector del ordenador. [...]

20. [\*LC CyberBlog » Blog Archive » EULAs and DRMs\*](#) Says:  
[November 10th, 2005 at 8:07 pm](#)

[...] The law suits filed this week against Sony that Dan mentions in his post from earlier today, will, undoubtedly delve into the legal import of these EULAs. If the consumer has consented to the installation of this program, in the form of the EULA, what legal claims remain? (on this point, check out Ed Felten's concerns part 1 and part 2). [...]

21. [\*The BillBlog » Blog Archive » The Rootkit of All Evil?\*](#) Says:  
[November 11th, 2005 at 9:48 am](#)

[...] Ed Felten comments: [www.freedom-to-tinker.com/?p=920](http://www.freedom-to-tinker.com/?p=920) Sony on XCP – watch this space  
[cp.sonybmj.com/xcp/](http://cp.sonybmj.com/xcp/) [...]

22. [\*Tom Ciarlone\*](#) Says:  
[November 14th, 2005 at 8:11 am](#)

Class Action Law Firm Investigating Sony CDs:

My law firm is investigating the situation surrounding "rootkits" on Sony-label CDs. In connection with our investigation, we are interested in learning more about the experiences consumers have had with those CDs. I can be contacted at (212) 239-4340 or, by e-mail, at [tcialrone@lawssb.com](mailto:tcialrone@lawssb.com).

23. *B C Says:*

[November 15th, 2005 at 12:25 am](#)

ZEROING IN ON "SPECIFIC HARM" MUSICK CD TROJAN HORSE:

Trojan Horse, May be called AWARE  
Installs AOL w/o permission to access internet.  
Found on Sony "CD EXTRA" format. Affects PC and Mac.

Trojan Horse defined: An ancient act of warfare in which  
the WALLED city of Troy was given a gift of a giant horse statue.  
When the gift was taken into the city,  
enemy soldiers came out of the horse and Destroyed the City.

"CD EXTRA" promises MORE FUN if you play the CD on a computer.

24. *Grey Bird Says:*

[November 17th, 2005 at 5:40 am](#)

To Tom: While Sony may have billions of dollars, if we (the billions of consumers worldwide) stop buying their CDs because of copy protection then they will stop putting copy protection on them because their billions come from... You guessed it: US!

Btw, a friend was trying to rip a CD on the contaminated list a couple of months ago before this fiasco came out. I figured that some kind of copy protection was why he couldn't rip it (well, the songs did copy but had some serious problems and were not listenable). I turned off autoplay on my machine and ripped them with no problem. The lesson: Autoplay is bad! Now I have to help him and another friend who tried to rip the disc for him get this rootkit off of their machines. (Mine, btw is clean according to rootkitrevealer by Sysinternals.)

25. *VibeBender Says:*

[November 17th, 2005 at 8:26 am](#)

This post and all the others that probably will result is one that I have seen and experienced first hand.....Integrity can be found on both sides.....and he with the most correct integrity will win the fight.....

26. [Side Channels » Blog Archive » Sony is pissing from the jumping board](#) Says:

[November 17th, 2005 at 3:23 pm](#)

[...] Very brief recap: Sony included malicious code with a handful of CD's. This code covertly installed itself on any computer the CD was inserted and put it in harm's way, especially when you use Sony's tool to remove it.  
[...]

27. *Anonymous Says:*

[November 21st, 2005 at 4:12 pm](#)

After one company sued a grandfather for more than \$5000 for downloading a movie, The individual copyright holders should be sued for damage to each machine. You cannot hire a computer professional for less than \$5000 to remove the faulty added software from a machine to restore it to the condition that existed before the disk asked for your agreement to its conditions....

28. *C C Says:*

[November 22nd, 2005 at 5:52 pm](#)

SonyBMGmusic.com just advertised CDs on NBC's late show, whether it was over the whole network or just locally I don't know. But I suppose it got plenty of well deserved whacking because their website is down. That gives me a little more confidence as the global media dyscombobulated-conglomeration is trying to whitewash this and apparently it's succeeding enough to attract some beastmarked investors. Unfortunately PLAYSTATION and VICE CITY type things and their addicts are a tape-patched inflatable lifesaver for them.

A certain factory shut down due to Windows BSOD recently. I can imagine worse industrial BSOD problems. Sure, solved by not listening to music and not running your factory on Windows. Here are other BSOD events I recently witnessed (which I assumed happened WITHOUT DRM)...

A bar couldn't serve drinks for an hour.

Disney World couldn't sell food for an hour.

Yes, there's a Windows Restaurant Edition(tm) or something like that, I witness.

What's sad about the factory shutdown is that the windows control panel cost almost a million dollars and replaced a 4 kilobyte paper tape reader that could have been fixed with a splice, and was in fact bought and used by another factory. It had been in constant use for 40 years. Divide the MTBF of windows by 40 and you're "better off" at a horse race.

And Sony has only revealed a few more CD titles with XCP, as far as I know they're not talking about the SunCom one or the one that SECRETLY installs AOL. SECRETLY means no EULA, no AOL logo on the CD, total malice and liability on their part. FYI the CD\_EXTRA format in general does this (there may be exceptions but not in my CD collection). You might find in the fine print "This CD includes free internet access" or something obscure like that, which looks more like a typo. Like "This phone includes free service".

How many have had the displeasure of un-installing AOL? Well, CD\_EXTRA is "rootkit enhanced by AOL", assuming optimistically that the versions of AOL-CDs that come every other day for free in the snailmail box don't include rootkits. Don't forget I am a victim of a Remote Control hack, and arbitrarily claim a lost-art exchange. The quitclaim requires PC replacements, not CD replacements. Not subject to any EULA because there was none, THE CDS ARE MINE.

WOULD YOU LIKE A FREE ROOTKIT, ANYONE? Just kidding about that.

Remember, they only have to stop it until "after the flu epidemic".

So said the Department of Homeland Security!

And maybe God. So, maybe only Sony will get the flu!

Quick, before I do, let's sing a new song...

When Sony Gets The Flu My Friends, hurrah hurrah...

...We'll all hear good tunes when Sony gets the Flu!

VIRUS MUSIC...HA!

As Arlo Guthrie said in Alice's Restaurant...

wait until it comes around again... it's coming around...

You can get anything you want at Alice's restaurant!

What if Sony COUGHS on the replacement CDs?

Let DRM be "Dead with Rigor Mortis". Avoid it like THE PLAGUE.

29. C C Says:

[November 23rd, 2005 at 1:08 am](#)

Let me clarify my position for that rant:

I am an artist and Sony "broke my guitar" and stole my art.

They are the PIRATES in this case. I was ROBBED!

Just for Playing, not Copying, one CD!

30. [Cheap cds](#) Says:  
[November 23rd, 2005 at 8:28 am](#)

I dont think copy protection can ever go to far. If you copy software or music or anything then its exactly the same as just walking into the shop and taking it off the shelf, its stealing whichever way ya look at it!

31. [Give it a rest](#) Says:  
[November 24th, 2005 at 11:56 pm](#)

Cheap cds, you are an idiot! And the kind of dolt that Sony wants on their side.

32. [RACCOONBILLY@AOL.COM](#) Says:  
[December 26th, 2005 at 7:25 am](#)

I BOUGHT A BMG CD "JANIS JOPLIN / BIG BROTHER LIVE AT WINTERLAND" BIG BROTHER WAS THE NAME OF HER BAND.  
 NOW IT ALSO MEANS THAT "BMG-BIG BROTHER" IS OUT TO RUIN YOUR COMPUTER. IN EARLY NOVEMBER MY WEBROOT-SPYSWEEPER CAUGHT SOME TYPE OF "ROOTKIT" RUNNING IN MY COMPUTER. BUT IT WAS FOUND "TOO LATE" AND THE THING FROM BMG RUINED MY COMPUTER.  
 ALL I DID WAS DOWNLOAD THE CD (I BOUGHT & PAID FOR) INTO MY COMPUTER FOR EASIER LOCATING & PLAYING. I MADE NO COPIES TO SEND OR BURN. SPYSWEEPER FOUND THIS "ROOTKIT" IN THAT JANIS JOPLIN CD STORED ON MY COMPTER. BE CAREFUL WITH CD YOU BUY & LOAD INTO YOUR COMPUTER. MY COMPUTER IS RUINED.

33. [GROKLAW](#) Says:  
[January 7th, 2006 at 5:20 pm](#)

[...] Meanwhile, antivirus firms are already warning about a new trojan in the wild taking advantage of the rootkit. This story raises some questions. These CDs with rootkits have been sold for 8 months. Where was Microsoft? Why didn't they and antivirus companies notice this rootkit themselves long ago? When the story first hit, here's the explanation given by First 4 Internet, the company that wrote the rootkit for Sony1 : The creator of the copy-protection software, a British company called First 4 Internet, said the cloaking mechanism was not a risk, and that its team worked closely with big antivirus companies such as Symantec to ensure that was the case. The cloaking function was aimed at making it difficult, though not impossible, to hack the content protection in ways that have been simple in similar products, the company said. So, Symantec and "the big antivirus companies" already knew about the rootkit? According to this statement, it seems they did. Are they then liable as well as Sony? Groklaw member alongmead asked another valid question in a comment to an earlier article: Does that mean that Microsoft knew also and was complicit, deliberately ignoring the rootkit? Alternatively, if not, might one not legitimately ask if Microsoft's anti-spyware is "sophisticated enough to detect the system changes" made by Sony's DRM? Which explanation is worse? I can't help but wonder about a third possibility. Charlie Demerjian recently wrote about what he views as the new Microsoft PR technique. He says because Microsoft lacks credibility, they don't put out press releases on certain stories. Instead they leak it to the press or to blogs. I'll let him describe it for you: MS has taken to 'slips', 'admissions' and 'leaks' in ways that it 'really should not have' done. The reporter pounces, and the Microsoft spokesperson gets all defensive and asks that it not be published, blah blah blah. Memos leaked to the right people have a similar effect, as do blog entries as a first line of press knowledge. Few things work better than a grass roots spreading of 'facts' that the mainstream press 'notices'. Few PR efforts or change of direction come in press releases any more, they all come from blogs and leaked memos. The people who pick the stories up and grassroots spread them tend not to mock as much as the real press. Those that do can be easily laughed off by real PR as the lunatic fringe. Basically, Microsoft is using the boggosphere to do its PR for them, and we are supposed to be the pawns. Is that what happened here? I have no idea, but I know it's the right question. I'm not in love with Sony at the moment, but fair is fair. I thought it was important to mention all this, because of the litigation. Just how deep does this betrayal of customers go? F-Secure, who was not part of the complicit agreement apparently and discovered the rootkit independently, according to Russinovich, explained on November 4 on their blog why rootkits are a security problem: A member of our IT security team pointed out quite chilling thought about what might happen if record companies continue adding rootkit based copy protection into their CDs. In order to hide from the

system a rootkit must interface with the OS on very low level and in those areas there's no room for error. It is hard enough to program something on that level, without having to worry about any other programs trying to do something with same parts of the OS. Thus if there would be two DRM rootkits on the same system trying to hook same APIs, the results would be highly unpredictable. Or actually, a system crash is quite predictable result in such situation. So imagine a situation where Joe Customer buys CD from label A and another CD from label B. Label A uses third party DRM from company X and Label B uses from company Y. Then our user first plays one of the CDs in his PC, and everything works fine. But after he starts playing the second CD, his computer crashes and won't boot again. This is something I would not like to associate with buying legal CDs. The Department of Homeland Security agrees. This IP protection is now threatening our security. How did everyone lose their sense of proportion? I earlier put a link to the audio of Stewart Baker, Department of Homeland Security Assistant Secretary for Policy, in News Picks, but what he said is so important, I wish to repeat it here: "It's very important to remember that it's your intellectual property — it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days. "If we have an avian flu outbreak here and it is even half as bad as the 1918 flu, we will be enormously dependent on being able to get remote access for a large number of people, and keeping the infrastructure functioning is going to be a matter of life and death and we take it very seriously as well." - DHS Ass't Sec'y on Policy Stewart Baker Copyright infringement is important to companies like Sony, of course, but if, when enforcing their rights, they end up exceeding their actual rights and endanger our lives in their quest to protect mere money, something is seriously out of balance. I also most sincerely hope that the DHS realizes the security value of the GNU/Linux operating system, as well as MacOSX. If the Department is relying exclusively on Windows, I am frankly terrified. By the way, if you'd like to hear the immortal words from Sony about rootkits and how customers don't know what they are and so needn't care about them, here you go. Your choices to listen to the audio are Windows Media Player or RealPlayer. Is it time, folks, for websites to broaden the choices they offer people? Some of us are afraid to use Windows, you know. And for any of you who are staring at your Windows computer and wondering just how bad it is in your personal case, may I encourage you to think about GNU/Linux systems as a remedy? It's one advantage of FOSS software that there is no code you are not allowed to examine. That's part of what the Free means in Free Software and the Open in Open Source, that you are free to look at the code and are free from secret corporate dirty tricks and private gentlemen's agreements that put your security at risk. [Note that the article referenced was later [at least by November 23, 2005] changed to read: "The creator of the copy-protection software, a British company called First 4 Internet, said the cloaking mechanism was not a risk. The company's team has worked regularly with big antivirus companies to ensure the safety of its software, and to make sure it is not picked up as a virus, he said." [...]]

34. [\*Ratiatum - Journal - Acculé, Sony BMG offre la solution anti rootkit\*](#) Says:  
January 8th, 2006 at 3:25 pm

[...] DADVSI : Jacques Chirac soutient son gouvernement Acculé, Sony BMG offre la solution anti rootkit  
Publié le Jeudi 03 novembre 2005, à 9H46 (+0100 GMT) Par Guillaume Champeau Sony BMG s'est à nouveau offert une belle cure d'impopularité en attaquant ses clients et non les pirates. Un expert en sécurité a découvert qu'un système malicieux avait été dissimulé dans son système par un CD de la maison de disques librement vendu dans le commerce. Foudroyée par toute la presse, Sony BMG a diffusé la solution pour s'en débarrasser. Mark Russinovich a provoqué un véritable raz de marée de colère contre la maison de disques Sony BMG. En testant la dernière version du logiciel RootkitRevealer, l'expert en sécurité de Sysinternals.com a découvert qu'après avoir joué le disque Get Right with the Man des frères Van Zant sur son ordinateur, "Sony avait installé sur [son] système un logiciel qui utilise les techniques communément employées par les malwares pour dissimuler leur présence". En termes d'experts : un rootkit. Selon Wikipedia, un rootkit est un "programme ou un ensemble de programmes permettant à un pirate de maintenir dans le temps un accès frauduleux à un système informatique". Sony aurait donc utilisé des techniques de pirates dans ses protections par DRM. Encore une fois, ce sont les procédés XCP de la société First 4 Internet qui font scandale. Sony BMG et EMI ont toutes les deux commercialisé des CD avec cette technologie de DRM, mais pour le moment seule Sony a été visée par l'affaire du rootkit. Sans doute la maison de disques germano-japonaise a-t-elle cru que tout était permis dans la lutte anti-piratage. Sans doute n'a-t-elle pas compris, surtout, que les systèmes de protection apposés sur les CD commercialisés n'affectent que les consommateurs les plus loyaux qui sortent leur portefeuille pour acheter de la musique. Les autres, ceux qui utilisent eMule ou Soulseek, peuvent télécharger les mêmes albums au format MP3 en étant totalement sûrs de ne pas se retrouver avec un rootkit sur leur PC. Et c'est un comble. Le principe de précaution s'applique-t-il aux CD ? Combien de fois l'industrie du disque a-t-elle accusée le P2P d'être

dangereux pour la sécurité des internautes, en pointant du nez spywares, malwares et autres virus ? Faut-il maintenant pointer du doigt les CD commercialisés comme étant dangereux pour la sécurité des consommateurs ? Selon First 4 Internet, le procédé ne présenterait aucun danger pour l'utilisateur, et il aurait même été abandonné par Sony. Mais quel système utilisent-ils aujourd'hui ? Le fait même de vouloir dissimuler un procédé sur le PC du consommateur honnête est intolérable. L'accord de licence que doit "signer" l'utilisateur est mensonger, et parce que le rootkit est mal conçu, toute tentative de supprimer les fichiers cachés risque d'endommager le système. "Le problème ça n'est pas qu'ils aient utilisé une méthode de rootkit en particulier. Le problème c'est tout simplement qu'ils aient utilisé des méthodes de rootkit", s'inquiète par ailleurs Edward Felten sur son blog. Le célèbre professeur a immédiatement demandé à Sony de sortir un patch pour désinstaller le rootkit. C'est chose faite. Dans un communiqué publié tête basse, la maison de disques affirmait hier que "le composant n'est pas malicieux et ne compromet pas la sécurité de l'ordinateur". Pour rassurer ses clients, Sony BMG indique tout de même l'adresse où télécharger le patch. Mais peut-on avoir confiance dans un patch proposé par les auteurs du rootkit ? La question relève bien sûr du réflexe paranoïaque. En période de chute des ventes de poulets pour pseudo risque de grippe aviaire, c'est un réflexe dans le vent. Pas de téléchargement pour Jean-Sébastien BachEMI et Nokia immobilisent la mobilité fonction HideChamps( champ ){ var Pdiv = document.getElementById( champ + '\_hidden' ); Pdiv.className = ( Pdiv.className == champ + '\_hidden' )? champ : champ + '\_hidden'; } 15 Commentaires (inverser l'ordre) Ajouter un commentaire Totoffe - le Mardi 08 novembre 2005, à 14H06 Moralité : Sous Windows, si vous insérez un CD, n'oubliez de maintenir la touche MAJ pendant 20 secondes, histoire de désactiver l'exécution automatique du contenu. Ne lisez que les pistes audio et surtout ne touchez pas aux exécutables de la piste de données. Après copy-protected sur la jaquette, va-t-il falloir que les majors ajoutent une étiquette "please scan with antivirus, antitrojan, antirootkit, antispyware, antimalware, antikeylogger, etc. before using this product" ? Sabinou - le Vendredi 04 novembre 2005, à 15H19 N'y aurait-il pas risque pour eux de subir un procès, car c'est bel et bien un acte de piratage... En tous cas, moi sous Linux, je vous dis pas le BIEN que ça fait d'avoir confiance en sa machine ^^ J'ai plus besoin de lancer spybot puis ad-aware puis pest patrol puis microsoft antispyware puis scanner mes trois quarts de teraoctet à l'antivirus, sur un PC ralenti pour des heures par le scan, et le reste du temps de toutes façons ralenti à mort par la protection temps-réel de pest patrol et de l'antivirus. Je me contente d'avoir mon pare-feu intelligemment configuré, et j'ai CONFIANCE dans mon système d'exploitation, je ne soupçonne pas par paranoïa mais avec un trop fort risque d'avoir raison malgré tout, d'avoir des saletés installées sans que je le sache. La confiance... quel bonheur 😊 ) fredoush - le Jeudi 03 novembre 2005, à 23H32 arg merde. business bussiness bizness bu... oh zut, qqun corrige moi! pis histoire de remplir ce post, un peu de propagande pour les systèmes libres (et propres: 0 spyware, 0 adware ni autres cadeau puant) : LINUX IS SEXY ! essaye ubuntu si tu as internet, mandriva sinon! <http://distrowatch.com> pour en essayer d'autres et trouver TA distribution GNU. fredoush - le Jeudi 03 novembre 2005, à 23H24 je suppose que je ne pourrais pas lire un cd 'protégé' par cette merde sur mon système GNU/Linux... enfin ça remet les choses en place ; combiné à d'autres faits du même accabité il apparaît que ceux qui sont VRAIMENT mal intentionnés/hors la loi/irrespectueux ne sont pas les 'copieurs' (oui c'est décidé - enfin pour l'instant - je n'emploie plus le mot de pirate pour tout ce qui a trait au malmenage du droit d'auteur) mais bien les faiseurs de morale. pis c'est marrant quand même, de voir qu'ils plombent leur business eux-même en donnant de bonnes raisons de préférer les mp3/ogg. comme si l'encombrement et la fragilité de leurs galettes en plastique ne suffisaient déjà pas! arf. arf. arf. à part ça évidemment il faut aimer les DRM et faire totalement confiance au RFID (c'est pour notre bien et ça te fera pas de mal!)... oui oui oui, mais bien sûr. Shivastudio - le Jeudi 03 novembre 2005, à 21H55 ça se désinstalle ... voir mes essais dans le forum <http://www.ratiatum.com/forum/index.php?showto> pic=47571 bye ! cyberpiv - le Jeudi 03 novembre 2005, à 17H20 Le fameux 'patch' ne propose en rien de désinstaller le rootkit, il propose juste de ne plus cacher les fichiers... Après, si tu veux le désinstaller, c'est une autre paire de manches... pHi - le Jeudi 03 novembre 2005, à 15H33 "les logiciels de p2p ne sont pas illégaux et ne compromettent pas la sécurité de l'industrie du disque" tiens c'est rigolo, ça marche aussi, comme ça... Blastm - le Jeudi 03 novembre 2005, à 12H49 "le composant n'est pas malicieux et ne compromet pas la sécurité de l'ordinateur". mais lol, c'est quoi un rootkit alors? ok, en lui-même, il attaque pas le système en lui-même; mais il ouvre des portes à d'autres programmes qui pourrons, eux, le faire. pHi - le Jeudi 03 novembre 2005, à 12H37 c'est combien d'années de taule, en france, déjà, piratage informatique en bande organisée ??? Oungawak - le Jeudi 03 novembre 2005, à 11H40 Babdunord: Arf c'est de ta faute aussi, tu as oublié le "!" . Comment veut tu comprendre son message si tu ne le lit même pas en entier ? Oungawak - le Jeudi 03 novembre 2005, à 11H38 jpyrat:Ben c'est normal. Si tu vire leur rootkit avec leur patch, faut bien qu'ils en installent un autre sinon comment il vont faire pour surveiller tes activités sur ton pc ? - - Quand les grosses boîtes se prennent pour des kevin r3b3lz... Babdunord - le Jeudi 03 novembre 2005, à 11H38 neo2004pf : comme je te l'indiquais dans un précédent commentaire, pourrais-tu m'éclairer sur la signification et

le sens profond de ton commentaire "PREUMS". Je suis sûr que ton explication me permettra de mieux appréhender toutes les composantes et les subtilités de ton intervention. Merci d'avance. neo2004pf - le Jeudi 03 novembre 2005, à 11H29 "le composant n'est pas malicieux et ne compromet pas la sécurité de l'ordinateur" Ils ont encore perdu une bonne occasion de la boucler, là ! Mark Russinovich (qui est expert en informatique) affirme le contraire. jpyrat - le Jeudi 03 novembre 2005, à 11H22 Incroyable : il faut Internet Explorer pour avoir le patch. Avec FireFox, on a cette page : <http://updates.xcp-aurora.com/unsupported.aspx> avec : XCP Support ActiveX Unsupported Sorry, your Internet Browser does not support ActiveX Controls. Please use Microsoft Internet Explorer to continue. Download Internet Explorer from the Microsoft website neo2004pf - le Jeudi 03 novembre 2005, à 11H01 PREUMS ! Ajouter un commentaire Vous devez vous inscrire pour ajouter un commentaire (inscription gratuite) var a\_fields = { 'comment': { 'l': 'Commentaire', 'r': true } }, o\_config = { 'to\_disable': [ 'Submit' ], 'alert': 1 } var v = new validator('form\_comment\_news', a\_fields, o\_config); Ratiatum.com : Abonnements | Syndication (RSS) | Publicité | A propos © Droits en partie réservés, PressTIC SARL. Données personnelles Technorati \_uacct = "UA-69689-1"; urchinTracker(); [...]

35. [Techdirt: Sony Says It Will Patch The Rootkit... Sort Of](#) Says:  
[January 10th, 2006 at 6:43 am](#)

[...] Search Techdirt Try the Advanced Search. Sony Says It Will Patch The Rootkit... Sort Of Contributed by Mike on Wednesday, November 2nd, 2005 @ 01:08PM from the too-little-too-late? dept. Sony BMG and First 4 Internet, the makers of the rootkit copy protection that's getting so much attention these days, have announced that they'll be releasing a patch to fix the problem, while also delivering a fix to various anti-virus firms to put into their tools as well. Note that this patch doesn't actually remove the copy protection or even make it that easy to uninstall. It just reveals the part that was hidden deeply in the computer. This isn't quite the response that folks like Ed Felten suggested they take. Also, no word on whether or not other labels that use the same tools, like Universal Music, will also be releasing the patch. << If You Want To Email-Bomb Your Ex-Employer In The UK, You Should Do It Soon | Reply | Threaded | BBC Accedes To Record Label Whining >> [...]

36. [myfreepaysite](#) Says:  
[March 6th, 2006 at 12:08 pm](#)

I live in my own little world. But it's okay; they know me here.

37. [Autorun](#) Says:  
[April 2nd, 2006 at 1:37 pm](#)

Yeah, nice post, if you interesting autorun template and template for autorun software, like autoplay media studio, try to [Autorun template](#)

## Leave a Reply

Name

Mail (will not be published)

Website

---

Submit Comment

---

Powered by [WordPress](#).  
[Entries \(RSS\)](#) | [Comments \(RSS\)](#).



This work is licensed under a [Creative Commons License](#).